CHAPTER

7

IP ROUTING IN WINDOWS 2000

After reading this chapter and completing the exercises, you will be able to:

- Describe the difference between interior and exterior routing protocols
- Describe the routing protocols supported by Windows 2000, including RIP and OSPF
- Configure static routing
- Configure demand-dial routing
- Manage and monitor border routing
- Manage and monitor interior routing
- Manage and monitor RIP and OSPF
- Manage, monitor, and troubleshoot network traffic

Internet Protocol (IP) routing is the method that the IP protocol uses to transfer data between computers on a network. In Windows 2000, the **Routing and Remote Access Service (RRAS)** supports IP routing. You learned about RRAS in Chapter 6, which mainly covered the remote access features it provides. This chapter looks at its routing features.

This chapter begins with an overview of IP routing. It examines different types of routing, routers, and routing protocols. It then covers the implementation of routing in Windows 2000, including the configuration of both static and demand-dial routing. Finally, the chapter examines techniques for managing, monitoring, and troubleshooting the various aspects of network routing.

ROUTING OVERVIEW

At its simplest, routing is the process of moving information along a path from a source to a destination on a network. On an IP network, the source and destinations are called hosts and the information is fragmented into small pieces called packets that are transferred between these hosts. When multiple IP networks are connected together, devices called routers help move information between these interconnected networks.

Direct Routing

Direct routing occurs when both the source and destination host are on the same network segment. Consider a small IP subnet with only three hosts (A, B, and C), all wired directly together, as shown in Figure 7-1.

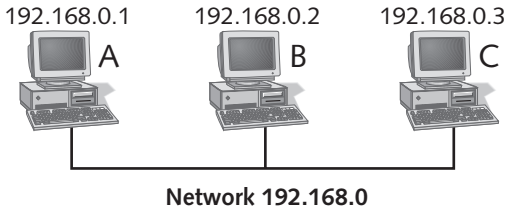

Figure 7-1 Single subnet

Many examples in this chapter assume that you are familiar with IP addressing and subnetting, concepts Chapter 2 of this book covers.

In Figure 7-1, the network ID for the subnet is 192.168.0 and Hosts A, B, and C have assigned host IDs of 1, 2, and 3, respectively. Now, suppose that Host A needs to send some information to Host C.

IP on Host A compares its network ID with the network ID of Host C. Since the two network IDs match, IP knows that the hosts are on the same subnet and that it can route the information directly to Host C.

Remember that although IP communicates using IP addresses, network hardware actually uses **MAC addresses**—the physical addresses of network interfaces—to communicate. This means that IP must have a way of translating, or resolving, an IP address into a MAC address. This happens through a portion of IP known as ARP, or **Address Resolution Protocol**. **ARP** is a low-level protocol that resides within IP. It provides a way of resolving IP addresses to MAC addresses. When a TCP/IP-based application needs to send information from one host to another, it segments and encapsulates that information into packets and tags those packets with the IP address of the destination host. ARP is then consulted to match that IP address to an actual MAC address. When ARP determines the MAC address, it gives that information back to IP and IP sends the packet on its way.

Indirect Routing

The procedure for direct routing works fine on a single network segment, but most large networks consist of smaller, connected networks and may also connect to the Internet. On these networks routing becomes a little more complex and is known as **indirect routing**.

Indirect routing takes place when the source and destination hosts are not on the same network segment and packets must pass through a router, a physical link between two or more networks. Routers are usually passive devices that do not pay attention to general network traffic. Packets destined for other networks must actually be sent directly to the router in order to be passed along, as Figure 7-2 shows.

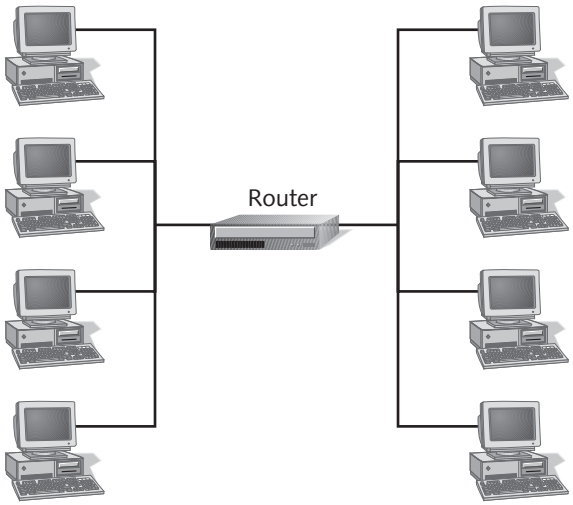

Figure 7-2 Sending packets across a router

You can actually think of a router as a computer with two or more network interface cards. Each card connects to a different network segment, and the computer can pass messages from one network to another.

Now, suppose that you take the single network segment just described and illustrated in Figure 7-1 and decide to connect another network to it, as shown in Figure 7-3.

The original network, shown on the left, has a network ID of 192.168.0. The second network, shown on the right, has a network ID of 192.168.1. The second network has three hosts, labeled L, M, and N. Hosts L, M, and N have host IDs of 1, 2, and 3, respectively.

A router labeled R1 joins these two networks. The router has two IP addresses, 192.168.0.25 and 192.168.1.25, because it has a separate interface on each network.

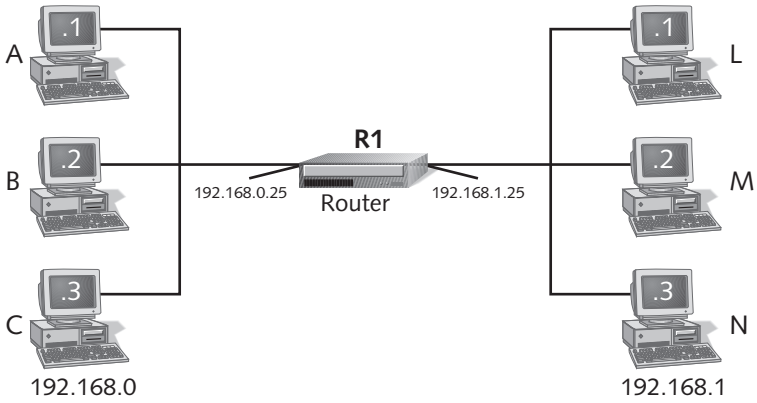

Figure 7-3 Two subnets connected by a router

Suppose now that Host A (192.168.0.1) needs to send a packet to Host N (192.68.1.3). The IP protocol on Host A examines the source and destination IP addresses and determines that the two hosts are on different network segments (because their network IDs do not match). IP now knows that this packet must be sent to a router.

IP determines the location of this router in one of two ways. IP first consults a locally maintained routing table. Figure 7-4 shows an example of this table, which is basically a list of networks that the system knows about and the IP addresses of routers that information must pass through to get to those networks. (The section entitled, "Static and Dynamic Routers," discusses routing tables in more detail.)

HSV-EXCH1 - IP Routing Table

Destination	Network mask	Gateway	Interface	Metric	Protocol
0.0.0.0	0.0.0.0	192.168.0.1	Local Area C...	1	Network ma...
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Local
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Local
172.16.204.0	255.255.255.0	172.16.204.1	Local Area C...	1	Local
172.16.204.1	255.255.255.255	127.0.0.1	Loopback	1	Local
172.16.255.255	255.255.255.255	172.16.204.1	Local Area C...	1	Local
192.168.0.0	255.255.255.0	192.168.0.200	Local Area C...	1	Local
192.168.0.200	255.255.255.255	127.0.0.1	Loopback	1	Local
192.168.5.0	255.255.255.0	192.168.0.200	Local Area C...	1	Static (non ...
192.168.8.0	255.255.255.0	192.168.0.200	Local Area C...	1	Static (non ...
224.0.0.0	240.0.0.0	192.168.0.200	Local Area C...	1	Local
224.0.0.0	240.0.0.0	172.16.204.1	Local Area C...	1	Local
255.255.255.255	255.255.255.255	192.168.0.200	Local Area C...	1	Local
255.255.255.255	255.255.255.255	172.16.204.1	Local Area C...	1	Local

Figure 7-4 Routing table, showing which gateway to use for each network address

If the network is not found in the static routing table, a default gateway is used. Defined on most TCP/IP hosts, the **default gateway** is simply a router where packets are sent if a destination network is not found in a routing table.

In this example, let's assume that Host A has its default gateway configured as 192.168.0.25, which is the network interface for Router R1. When IP determines that the packet destined for Host N needs to go to another network segment and it does not find the network in a routing table, it sends that packet to router R1.

ARP is still used in indirect routing but in a slightly different way. A packet destined for a remote network must be sent to a router. IP sends that packet using the router's IP address, but even the router's IP address must be resolved into a MAC address before the packet can be delivered. ARP resolves the router's IP address into a MAC address and the packet is sent. That router then determines whether to put the packet on another local subnet it connects to or to direct the packet to another router. Either way, its own IP must use ARP to establish the MAC address of the host to receive the packet.

In Figure 7-4, Router R1 directly connected to Network 192.168.1 and could forward the packet directly to Host N. It is possible, however, to create even more complicated networks where routers must send packets to other routers, as shown in Figure 7-5.

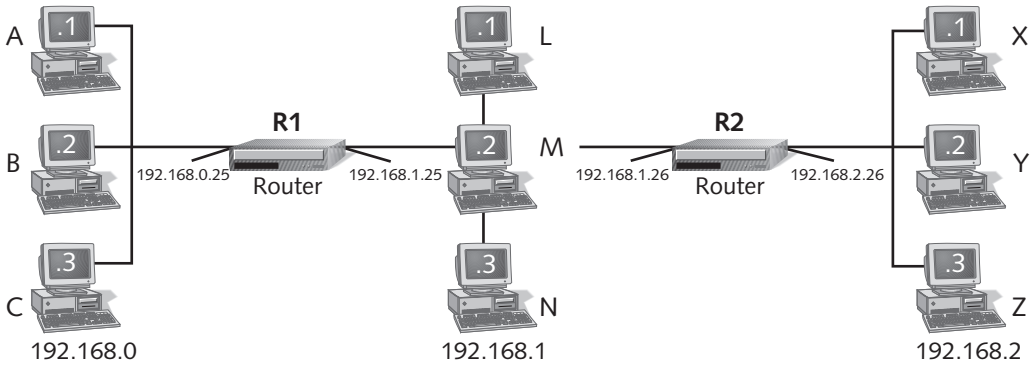

Figure 7-5 Three subnets connected by two routers

Figure 7-5 shows a third network added using Router R2. Suppose here that Host A (192.168.0.1) needs to send a packet to Host Z (192.168.2.3). As before, Host A determines that it must send the packet to another network segment and forwards the packet to Router R1 (its default gateway). This time, however, Router R1 does not directly connect to the destination network. Router R1 must forward the packet to another router, R2, whose address is again determined through a routing table or by using a default gateway. Router R2 directly connects to the destination network and can forward the packet straight to Host Z.

As you can see, routing can quickly become quite complex. The Internet itself is just a series of networks of varying complexity, each connected to one another using routers.

Static and Dynamic Routers

A router is a physical device used to connect a number of network segments together. Routers can be dedicated pieces of hardware whose sole purpose is being a router, or they can be computers that have more than one network adapter card, each connected to a different network segment. Computers configured this way are called **multihomed**. Most routers can have an interface on many different networks at the same time.

As mentioned in the previous section, when a router receives a packet from a sending host, it does one of two things. If the router is directly connected to the destination network, it can send the packet straight to the destination host. If the router is not directly connected to the destination network, it forwards that packet to another router, which then makes a similar decision.

Routers can do this because they maintain local routing tables that IP can consult for routing information. A **routing table** is basically a list of networks on the internetwork and the adjacent routers used to get to those networks. All routers have routing tables, but routers handle entries in these tables in a couple of ways. For the purposes of this discussion, routers are of two basic types: static and dynamic.

Static Routers

On a **static router**, you must enter routing tables manually. A static router only knows about networks that directly connect to it or networks that you tell it about. Consider the illustration in Figure 7-6.

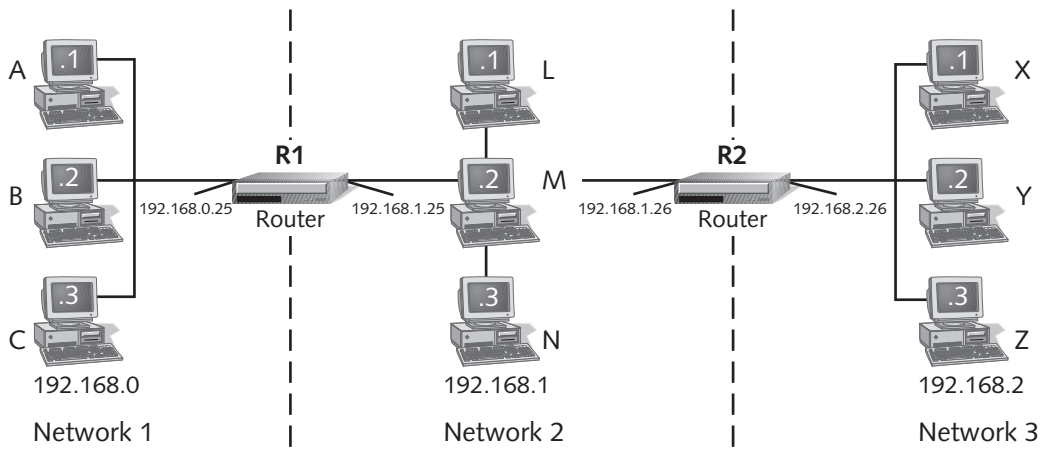

Figure 7-6 Subnets connected without routing tables

Here three small networks connect to one another using two static routers, R1 and R2. Router R1 only connects directly to Networks 192.168.0 and 192.168.1. Router R2 only connects directly to Networks 192.168.1 and 192.168.2. This means that, by default, Network 1 and Network 2 can communicate and Network 2 and Network 3 can communicate. However, Network 1 and Network 3 cannot.

In order to allow a static router to communicate with networks to which it is not directly attached, you can use one of two methods:

- Provide an entry in the routing table for every network on the internetwork.
- Configure each router with a default gateway (which will be the address of an adjacent router).

You must configure static routing tables manually and must include all known networks on the internetwork in order for the tables to work efficiently. Consider the configuration shown in Figure 7-7.

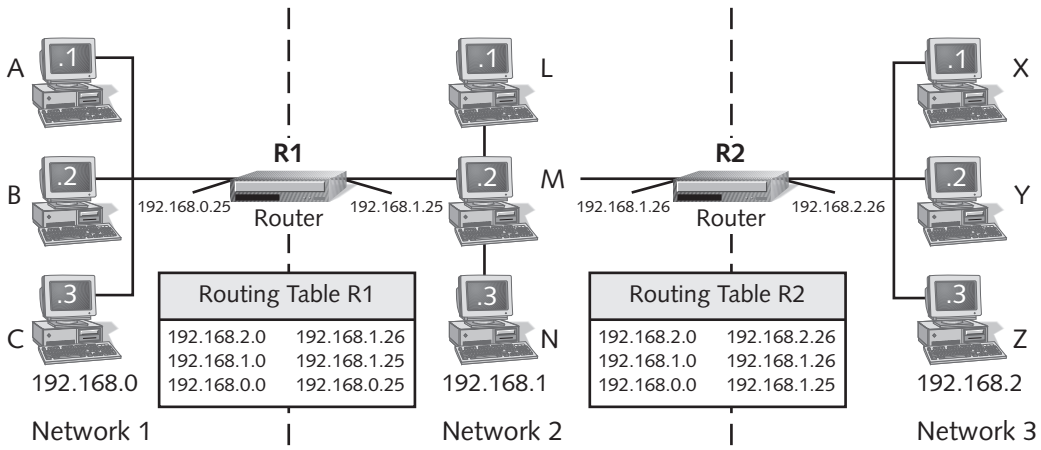

Figure 7-7 Subnets connected with routing tables

This example shows routing tables added to each of the routers. In the table for router R1, notice the first entry. The left column describes the network ID (192.168.2.0) for Network 3. The right column defines the IP address (192.168.1.26) to which router R1 forwards packets destined for that network. Through this one simple entry, Network 1 can now communicate with Network 3. The third entry in the table for router R2 allows Network 3 to communicate with Network 1.

All static routing table entries include the following information:

- *Network address*: network ID or network name of the network where packets might be sent
- *NetMask*: subnet mask for the corresponding network
- *Gateway address*: IP address where packets destined for the corresponding network should be forwarded

Dynamic Routers

As you can see, managing static routers on a complex network could require considerable time. Fortunately, larger networks use some form of **dynamic router**. Dynamic routers are simply routers having some automatic method of sharing their routing information with other routers on the network. If routing or network information changes, a router automatically updates its routing tables and forwards that information to other dynamic routers that it knows about.

When all routers on an internetwork have the correct routing information in their tables, the network has **converged**. When a link or router fails, all routers on the network must reconfigure themselves with the proper information. The time needed to do this is called the **convergence time** of a network.

Several protocols provide dynamic routing, the two most popular being Routing Information Protocol (RIP) and Open Shortest Path First (OSPF). The next section examines these and other types of routing protocols.

Routing Protocols

A routing protocol is a standard language that lets routers exchange routing information, freeing the administrator from the hassle of maintaining static routing tables. The following sections describe and provide examples of the two basic types of routing protocols: interior and exterior.

Before learning about interior and exterior protocols, though, you need to be familiar with another concept: the **autonomous system**. Loosely defined, an autonomous system is one with a set of networks and routers all under the same administration. For example, a corporate LAN that was segmented into many different subnets with routers is an autonomous system because it is administered separately from any other networks (such as the Internet) that it may connect to.

Interior Routing Protocols

A routing protocol used to connect two routers in the same autonomous system is called an interior routing protocol. Windows 2000 supports two interior routing protocols: **Routing Information Protocol (RIP)** and **Open Shortest Path First (OSPF)**.

Routing Information Protocol By far the most common interior routing protocol in use today is Routing Information Protocol (RIP). RIP is a distance vector routing program, meaning that it not only supplies information about the networks a router can reach, but information about the distances to these networks as well. This distance simply reflects the number of routers a packet must cross, or **hop**, in order to reach a particular network. This distance is referred to as a hop count, or sometimes as a metric. The maximum hop count allowed in RIP is 15. Any network with a hop count of 16 or greater is always considered unreachable. Routers use hop counts to determine the best route to use for a given packet at a given time.

The way RIP works is fairly simple. At a given interval (30 seconds is the default on a Windows NT router), a RIP-enabled router broadcasts (or multicasts, depending on the version of RIP) its routing table to the network. RIP-enabled routers receiving this broadcast add the routing information to their own tables, increasing the hop counts to each network by one in order to account for crossing the router that sent the broadcast. If the receiving router already has a route to any particular network, it compares routes and keeps only the one with the smallest hop count.

As of this writing, Windows 2000 supports both versions of RIP (RIPv1 and RIPv2). **RIPv1** is simple to use and well-supported, but requires a few considerations:

- Since each router maintains a list of all networks up to 15 hop counts away, routing table sizes can grow quite large on a complicated network. This means that routers need to be more powerful to handle the large table sizes.
- Every RIPv1-enabled router makes a MAC-level broadcast every 30 seconds. On internetworks with many routers, broadcast traffic volume can actually grow quite high.
- RIPv1-enabled routers give entries received from other routers a three-minute life span or time to live (TTL). If it does not receive a new broadcast from that other router within three minutes, the RIPv1-enabled router removes the entries from that router. When a router goes down, therefore, propagating accurate changes throughout the network can take some time.
- Because RIPv1 does not include the subnet mask along with its routing announcements, routers must try to determine the network ID using limited information. As a result, routers often incorrectly assume the default subnet mask.

RIPv2, the latest version of the protocol, addresses many of these shortcomings. While still limited to 15 hops, RIPv2 does provide a multicast option in addition to broadcasts for routing announcements and includes the subnet mask. In addition, RIPv2 now supports the authentication of incoming announcements from other routers.

Open Shortest Path First A link-state routing protocol, Open Shortest Path First (OSPF) enables routers to exchange routing information. It is called a link-state protocol because it actually creates a map (a routing table) of the network that calculates the best possible path to each network segment by maintaining information on the state of links (whether they are up or down).

To help keep this routing table from growing too large, OSPF divides the internetwork into collections of contiguous networks called **areas**, as shown in Figure 7-8. Each router only keeps a link state database for those areas connected to the router. Areas are connected to one another via a special type of area called a **backbone area**. Any router inside a backbone area is called a **backbone router**. Routers with interfaces on more than one area are called **area border routers**.

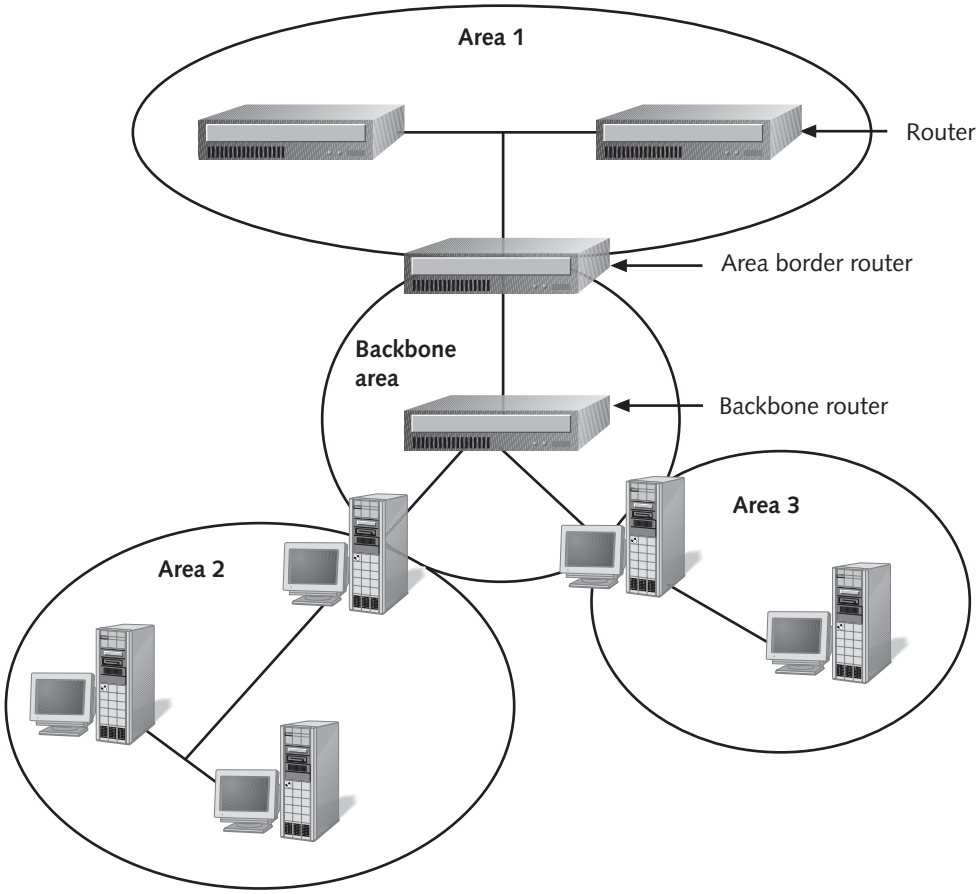

Figure 7-8 OSPF routers grouped into areas

One of OSPF's biggest advantages over either version of RIP is a lower convergence time, since it was designed specifically to maintain link-state tables. OSPF's primary disadvantage is that it is usually much more difficult to plan and configure than RIP.

Exterior Routing Protocols

Exterior routing protocols are used to exchange routing information between networks that are not autonomous (that is, do not share a common administration). The first exterior routing protocol developed was the **Exterior Gateway Protocol (EGP)**. Since then, a newer and more powerful exterior routing protocol has been developed named the **Border Gateway Protocol (BGP)**. Now in its fourth version, this protocol is often called BGP4. Windows 2000 RRAS does not support any external routing protocols, so this book does not provide any configuration information. It is important, however, to be aware that these protocols exist and their purpose.

Actually, you can use BGP as either an internal or exterior routing protocol, so you may often see it called internal BGP (IBGP) and external BGP (EBGP). Since Windows 2000 does not support exterior routing protocols, a full discussion of the BGP protocol is beyond the scope of this book.

Installing and Configuring RRAS

Now that you understand the concepts behind routing, it's time to see how it actually works on a Windows 2000 system. The first step in configuring a Windows 2000 server as a router is to install the Routing and Remote Access Service (RRAS) on the server. Actually, as you may remember from Chapter 6, RRAS is automatically installed along with Windows 2000 Server, but left disabled. All you need to do is enable it.

This section provides an overview of the set-up process and the choices you make. Hands-on Project 7-1 at the end of this chapter walks you through the actual steps of setting up RRAS as a network router.

First, you must log on to the server with Administrator privileges and open the Routing and Remote Access utility from the Administrative Tools program group on the Start menu. Shown in Figure 7-9, this utility is actually a snap-in for the Microsoft Management Console used to control most of Windows 2000 management features.

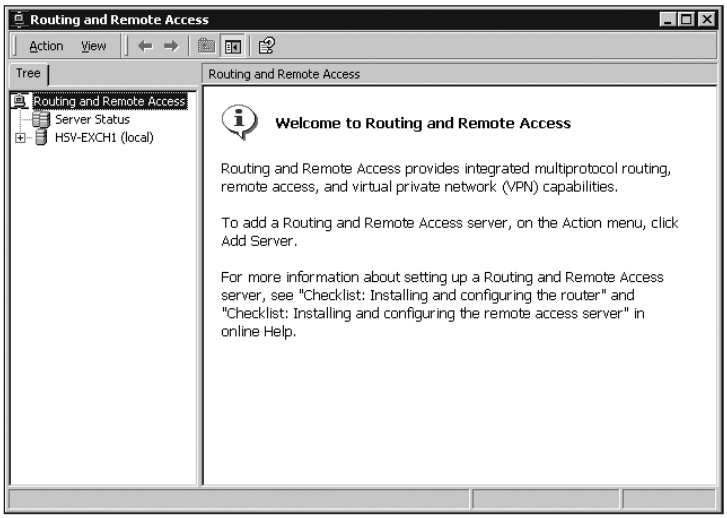

Figure 7-9 Routing and Remote Access snap-in

In the list in the left pane, find the name of the server and right-click it. From the shortcut menu that appears, choose the Configure and Enable Routing and Remote Access command to begin the Routing and Remote Access Server Setup Wizard. The wizard takes you through several configuration steps. The first, shown in Figure 7-10, asks you to select the

type of configuration you want to install. Choose the Network Router option. For details on what some of the other options mean, see Chapter 6.

Figure 7-10 Selecting a type of router to configure

Next, the RRAS Setup Wizard asks you to verify that the protocols you wish to use on the server are already installed and configured. If not, you must configure them before taking the next steps with the wizard.

The next page that you see asks you whether you want to configure the server to use demand-dial connections or not. If you elect not to allow them, you see a summary page for the wizard where you can just click Finish. If you choose to allow demand-dial connections, you must complete one more step before you finish: deciding whether to use DHCP or to define a static pool of IP addresses for remote clients. You see, when you enable demand-dial routing, you are essentially configuring a remote access server. Even if you do not plan to allow remote users to dial in to the server, other routers must have the option of connecting to it as needed. If you have a DHCP server on the same subnet as the RRAS server, the DHCP option is usually the best option. You learn more about configuring demand-dial connections later in this chapter, and you can find information on integrating DHCP with RRAS in Chapter 6.

And that's all there is to it. When the summary screen of the wizard appears, it reminds you that you still need to do a few things to create a working router:

- You must add **demand-dial interfaces** that can dial a remote router whenever a connection needs to be made and supports demand-dial routing.
- You must install and configure any routing protocols (RIP or OSPF) if you want your new router to function as a dynamic router. If you do not, you can configure static routing instead. You do not need to install any routing protocols in order for your RRAS server to be a functional router.

- You must give each routable interface on the server (network adapter card or demand-dial) a network address for each protocol you allow to be used over the interface. (This chapter discusses IP only.)

Once you exit the wizard, your RRAS server is set up and ready to start routing. Figure 7-11 shows the basic Routing and Remote Access snap-in window.

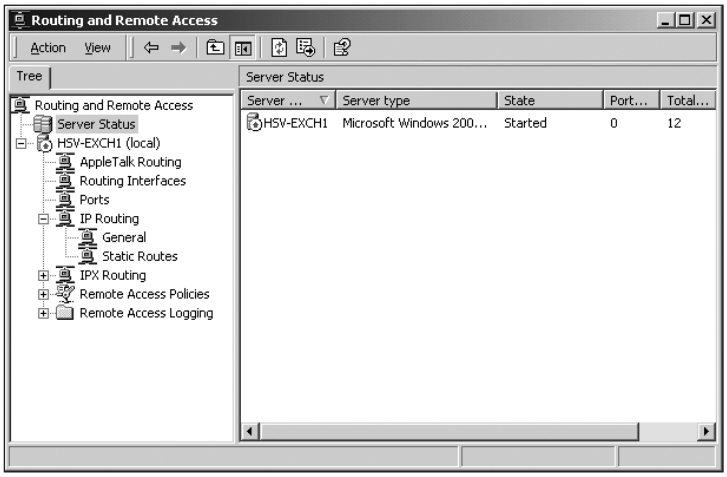

Figure 7-11 RRAS snap-in after RRAS is enabled

Chapter 6 covered most of the topics related to the management of the RRAS server, so we won't rehash it here. Instead, the following presents a brief management recap:

- Click the Server Status container to view the status of the server in the right pane. Status information includes the name of the server, whether it's running or not, the number of ports configured on it, and so on.
- Directly below the Server Status container is a container for a server, identified by the server's NetBIOS name. If more than one RRAS server is configured on the network, you see a list of server containers to choose from. Right-click the Server container (HSV-EXCH1 in Figure 7-11), and choose Properties from the shortcut menu to access a number of configuration parameters for the server. Chapter 6 details all these, but the important one to note here is the Router option on the General page. Use this option to turn the router on and off.
- Inside the server container, you see a number of containers named IP Routing, IPX Routing, and AppleTalk Routing. These containers hold different configuration objects, depending on the protocol. This chapter discusses the IP Routing container later.
- The Routing Interfaces container displays information on all routing interfaces configured on the server.

CONFIGURING STATIC ROUTING

When you enable RRAS on a server, routing turns on by default for each protocol configured on the server. This means that the server begins passing data packets immediately if clients are configured to use one of its interfaces as a default gateway. If the RRAS server is the only server on your network, or if you just don't want to set it up as a dynamic router, you do not need to install any routing protocols. Your RRAS server can function perfectly well as a static router. Of course, you have to update the routing tables yourself.

You can update static routing tables on an RRAS server in two ways: using the ROUTE command and using the RRAS snap-in.

Managing Static Routes with the Route Command

You use the **ROUTE command** to manipulate static entries in a routing table. The format for the route command is as follows:

```
Route [-f] [-p] [command [destination] [netmask] [gateway]
[metric]]
```

Table 7-1 defines the options you may use with the ROUTE command.

Table 7-1 Switches for the ROUTE command

Switch	Action
-f	Flushes all entries from the routing table
-p	Used with the ADD command to make a route persistent; used with the PRINT command to display all persistent routes
Command	Add, Delete, or Change (see the next three table entries)
Add	Adds a route to the routing table
Delete	Deletes a route from the routing table
Change	Changes a gateway address for a route that already exists
Destination	Network ID to which packets might be sent
Netmask	Subnet mask that tells IP how to calculate the network ID
Gateway	IP address where packets for the network being entered are sent; if the router is attached to this network, the address is one of the router's own interfaces; otherwise, it is the IP address of another router.
Metric	Hop count used in determining the route a packet takes

For example, entering ROUTE PRINT on the command line displays the contents of the current routing table. This should look something like Figure 7-12.

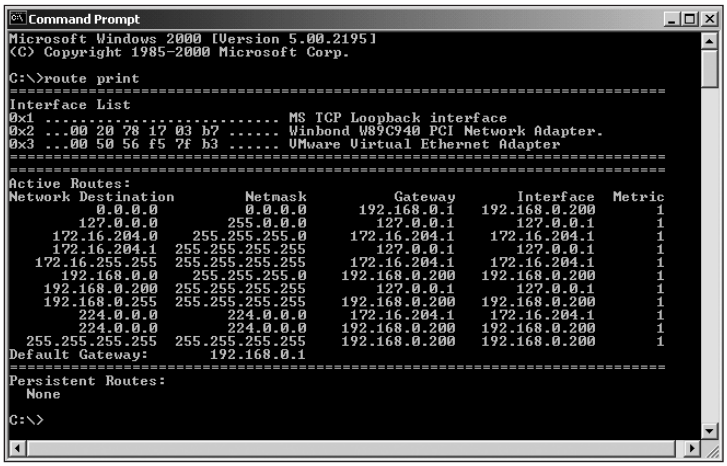

Figure 7-12 ROUTE PRINT command

Note the several entries in the table shown in Figure 7-12. Windows 2000 routing tables maintain the following default values:

- *Default route (0.0.0.0)*: route used for any network not specified in the routing table
- *Subnet Broadcast (255.255.255.255)*: address used for broadcasting to all nodes on the local subnet
- *Network Broadcast*: address used for broadcasting to all nodes on the internetwork
- *Local Loopback (127.0.0.0)*: address used for testing IP configurations and connections
- *Local Network*: address used to direct packets to nodes on the local network
- *Local Host:* address of local computer

Managing Static Routes with RRAS

While the ROUTE command is the traditional way of managing static routing tables (and useful to understand), the RRAS snap-in provides a much easier and less error-prone way. Hands-on Project 7-2 at the end of the chapter outlines the steps for adding and removing a static route from the routing table with RRAS. This section provides a brief overview of the process.

To view the routing table, first navigate to and highlight the Static Routes container inside the IP Routing container. The right pane shows any static routes that you added manually. (See Figure 7-13.) This pane shows none of the default routes configured by Windows 2000; however, don't be surprised if you find it empty the first time you look.

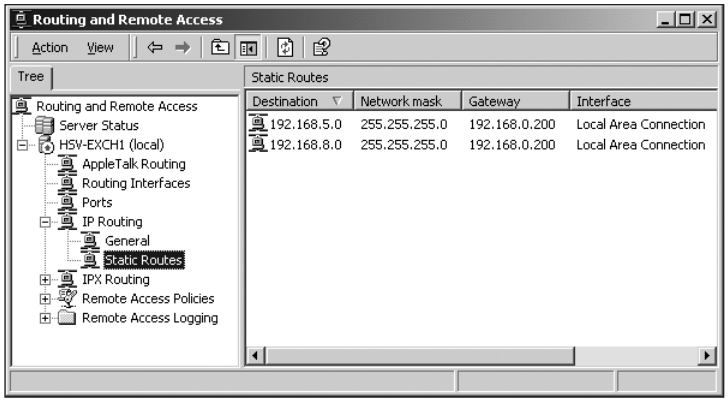

Figure 7-13 Viewing manually added static routes in RRAS

You can right-click any route in the right pane and select Delete from the shortcut menu to remove it from the routing table. Another way to view the routing table is to right-click the Static Routes container and choose the Show IP Routing Table command from its shortcut menu. This opens a dialog box similar to the one in Figure 7-14 that shows all routes in the table, including the default routes. You cannot manage routes from this dialog box, however. It's only there for looking.

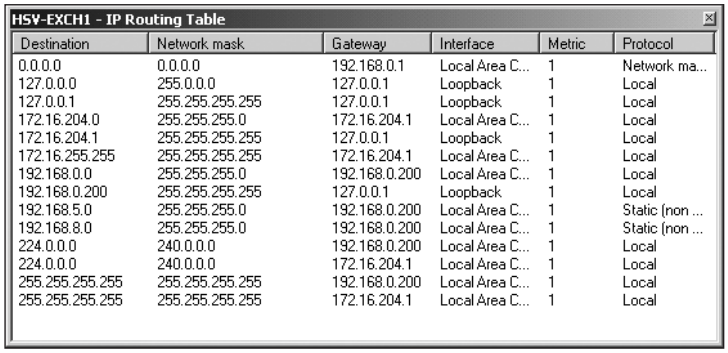

Figure 7-14 Viewing the full static route table in RRAS

To add a route to the table, right-click the Static Routes container and select the New Static Route command from the shortcut menu. This opens a dialog box like the one in Figure 7-15. Select the interface for which you want to create the route, specify a destination network and subnet mask, enter a gateway, and configure the number of metric hops allowed to reach the destination.

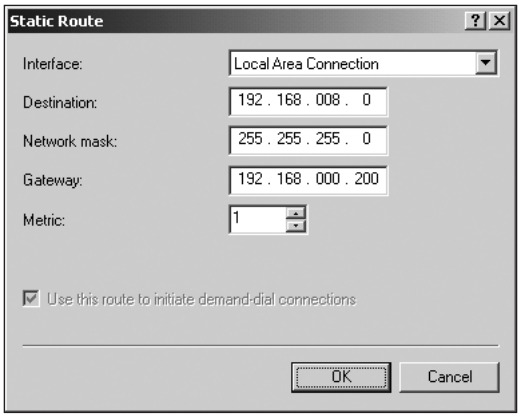

Figure 7-15 Adding a static route in RRAS

Using Dynamic Routing Protocols

If you find managing static routing tables not to your liking, or if you must manage large number of routers, you'll be glad to know that dynamic routing protocols are actually pretty easy to set up and configure. Once you decide between using RIP and OSPF (or both) and install the actual protocol, the protocol engine itself takes care of exchange routes with other routers it can find. In fact, you cannot even edit the contents of a dynamic routing table.

Whichever protocol you decide to use, the procedure for installing it is the same. Hands-on Project 7-3 at the end of the chapter provides a step-by-step look at the installation, but here's a brief rundown. First, find the IP Routing container inside the server for which you want to install the protocol. Inside that container, right-click the General container and select the New Routing Protocol command from the shortcut menu. Select the protocol you want and click OK. This installs the protocol and adds the new container for the protocol inside the IP Routing container. All you need to do is configure it.

Configuring RIP

There is really not much to configure for the RIP protocol. Once you install the protocol, RIP pretty much takes care of itself by looking for other RIP routers on the network and exchanging information with them. To configure what is available, right-click the new RIP container and choose Properties from the shortcut menu. There are two property pages available for configuration: General and Security.

General Properties

The General property page for the RIP protocol, shown in Figure 7-16, makes two properties available for configuration. The first is the maximum delay (in seconds) for how long a router waits to send an update notification to its peers. The second property is the level of event logging that the RIP protocol should perform.

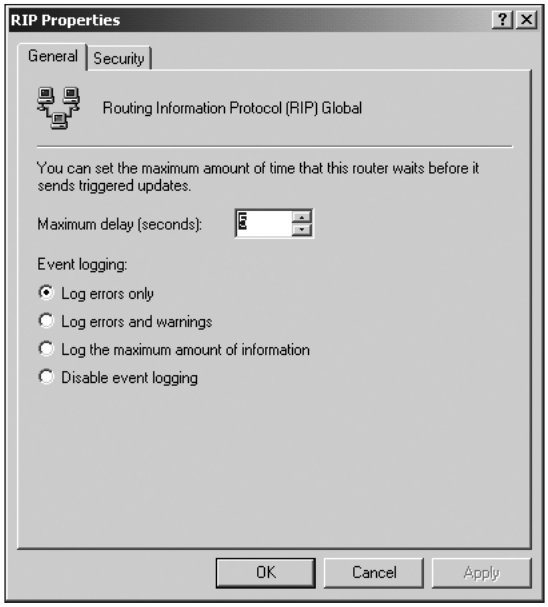

Figure 7-16 General property page for the RIP protocol

Security Properties

The Security page for RIP, shown in Figure 7-17, lets you select properties that control what router announcements your router accepts from other routers. By default, the router accepts all announcements, but you have the option of creating a list of routers whose announcements your router accepts or rejects.

Configuring OSPF

In the same way that you set RIP properties, you can also set many OSPF properties by opening the property pages for the OSPF container. Table 7-2 lists the available property pages and describes their general use.

While it may seem that this chapter glosses over the OSPF properties you can set, much of this information is too detailed to be presented here and not prominently featured on the exam. It's important to know some of the features available and generally where to configure them, but you do not need to get mired in the specifics of the OSPF protocol.

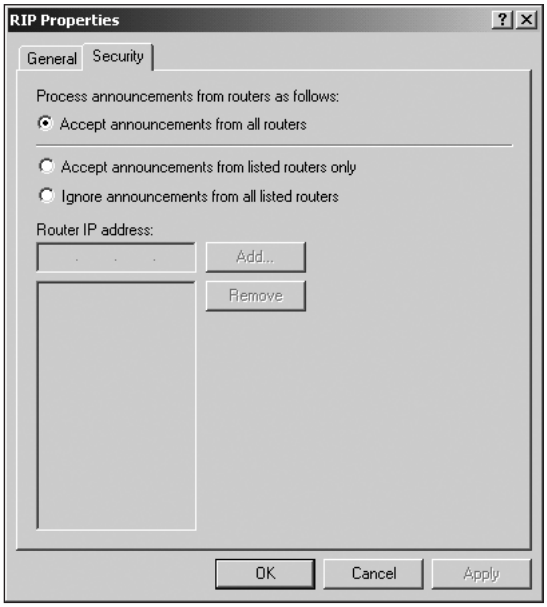

Figure 7-17 Security page for the RIP protocol

Table 7-2 Property pages for the OSPF protocol

Property page	Properties
General	Lets you configure the level of logging that the OSPF protocol performs, plus two other parameters: a Router Identification lets you enter an IP address that your router uses to identify itself; Enable Autonomous System Boundary controls whether your OSPF router advertises routers it finds outside your system
Areas	Lists the OSPF areas that your router knows about; you can add, edit, or remove areas from the list on this page; areas were discussed earlier in this chapter
Virtual Interfaces	OSPF divides routers into areas, some backbone areas and other regular areas; virtual links are used to configure non-backbone routers to exchange information with backbone routers
External Routing	Quite possibly your OSPF router can acquire routes from a number of sources besides other OSPF routers, including RIP routers and static routes; the External Routing page lets you control which external sources can add routes to the OSPF router

Working with Interfaces

Once you install and configure dynamic routing protocols, the next step is to add the interfaces (network adapters, demand-dial interfaces, and so forth) you want to use with those protocols. You must add at least two interfaces to each protocol. After all, the router is there

to accept traffic on one interface and send it out over another. That's what routing is. You can add as many interfaces as you have to a protocol, but adding all available interfaces is not necessary.

Actually, you are not really adding a new interface. You are taking an existing interface on the RRAS server and binding it to the protocol. However, Microsoft calls this adding an interface, so who are we to argue?

Managing LAN Interfaces

Before you start adding interfaces to protocols, it may be helpful to look at the properties you can configure for the LAN interfaces themselves. First, expand the IP Routing container and highlight the General container. This displays a list of LAN interfaces in the right pane, as shown in Figure 7-18.

You can also see a list of LAN interfaces in the Routing Interfaces container directly under the server container, but you cannot open the properties of the interfaces there. You must go to the General container to do this. Go figure.

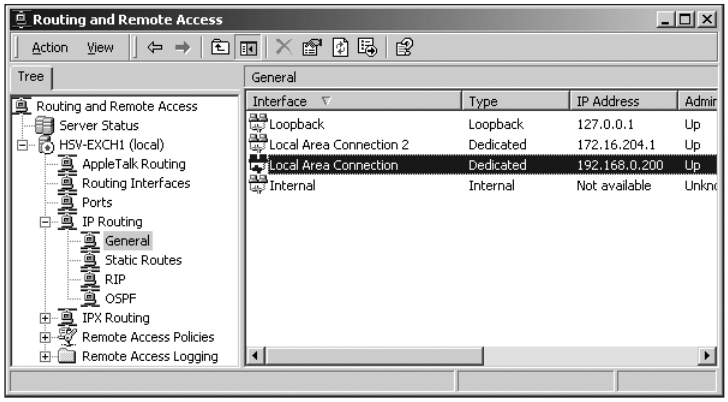

Figure 7-18 Viewing LAN interfaces in RRAS

Right-click any LAN interface and click Properties to open the property pages for that interface. There are four property pages presented: General, Configuration, Multicast Boundaries, and Multicast Heartbeat. The two that involve multicasting are beyond the scope of this book and the exam, and are not covered here. The next sections discuss the other two pages.

General Properties

The General page shown in Figure 7-19, lets you set properties for the entire interface. These include the following:

- *Enable IP router manager*: controls whether this interface allows IP routing. When disabled, the interface does not route packets and other routers cannot exchange information with it.

- *Enable Router Discovery Advertisements*: controls whether the router broadcasts router discovery messages. These are the messages used to find neighboring routers automatically. With this option enabled, you can also configure how long advertisements are valid, the preference level assigned to those advertisements (clients use routers with higher preferences first), and the minimum and maximum intervals for sending advertisements.
- *Input Filters and Output Filters*: let you selectively accept or reject packets on the interface. For example, you could create a filter that rejects all packets from a specified network address.
- *Enable fragmentation checking*: lets your router reject fragmented packets. With this option disabled, the router must accept and try to process fragmented packets. Sending fragmented packets is a popular form of denial-of-service attack on routers.

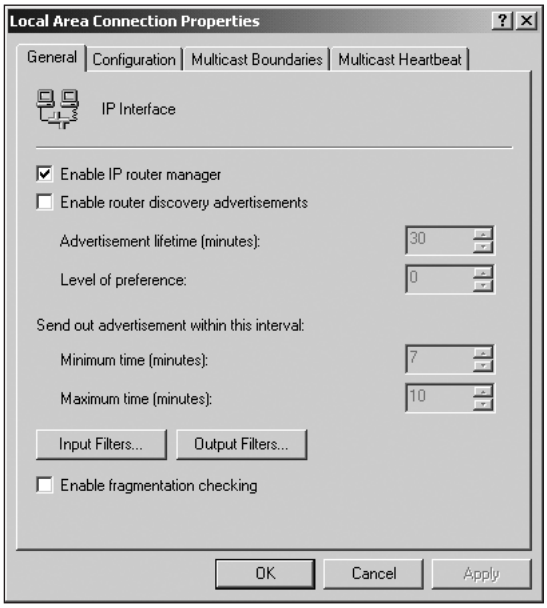

Figure 7-19 General page of a LAN interface

Configuration Properties

You use the Configuration page shown in Figure 7-20, to specify whether the interface should have static IP addressing information or receive it automatically from a DHCP server.

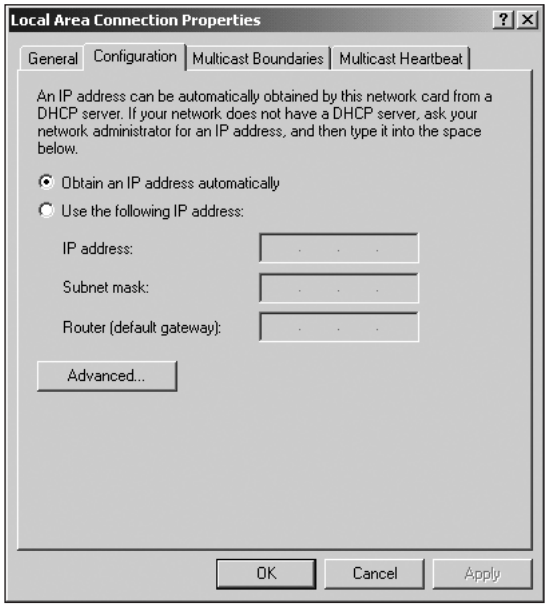

Figure 7-20 Configuration page of a LAN interface

Demand-dial Routing Interfaces

When you install RRAS, it automatically configures all the LAN connections that it can find. However, you must configure any demand-dial interfaces on your own. To start creating a demand-dial interface, right-click the Routing Interfaces container in RRAS and choose New Demand-Dial Interface from the shortcut menu. Hands-on Project 7-4 at the end of the chapter provides step-by-step instructions for creating a new demand-dial interface.

Here is a list of the basic steps involved in creating the interface:

1. Name the interface.

   If possible, choose a name that represents both the source and destination of the connection.

2. Choose a connection type.

   You can choose either a physical connection (modem, ISDN, and so forth) or a Virtual Private Networking connection. The choices for the rest of the wizard differ slightly depending on the choice you make here. Chapter 6 details the creation of a VPN connection, so we just focus on the physical connection here.

3. Choose the actual physical device for the interface.

   Since you cannot add a device from within this wizard, you need to set up any devices beforehand.

4. Enter a phone number for the connection.

   This is the number of the remote router.

5. Set routing and security options.

   Figure 7-21 shows this dialog. You can enable or disable the IP and IPX protocols for the connection, as well as establish some security guidelines. These guidelines include whether to add a user account so a remote user can dial in (selecting this adds another page to the wizard where you can fill in user information); allowing plain text passwords if you cannot use a more secure authentication, and using a script to complete the connection with the remote router (some routers require this).

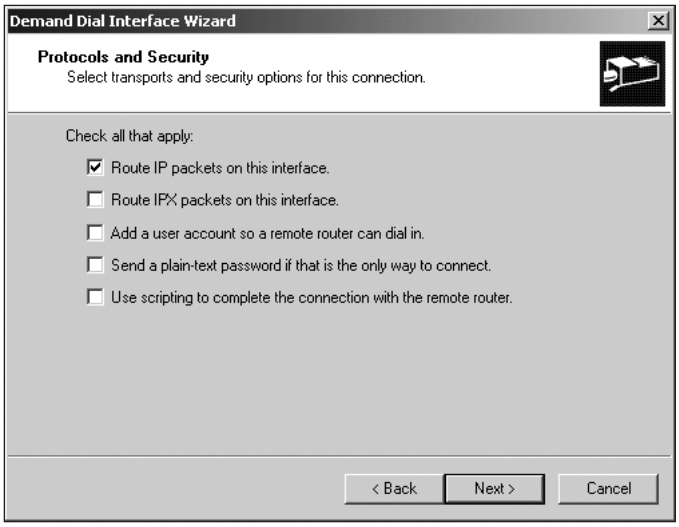

Figure 7-21 Routing and security options for a new demand-dial interface

6. Establish dial-out credentials.

   This includes any user information that your router needs to connect to and authenticate itself with the remote router.

Adding a LAN Interface to a Protocol

To add a LAN interface to a protocol, simply right-click the protocol container (for example, the RIP container) and choose the New Interface command from the shortcut menu. A dialog box opens that lists the available interfaces. Choose one and click OK to create the new interface. As soon as you create the new interface, you immediately see the property page for the interface. You can also configure these properties later by right-clicking the interface inside the protocol container and choosing Properties from the shortcut menu. The property pages for the RIP and OSPF protocols differ a bit, and the following sections discuss each.

RIP Interface Properties

Four pages with dialog boxes are available on interfaces attached to the RIP protocol: General, Security, Neighbors, and Advanced.

General Properties The General page for the RIP interface, shown in Figure 7-22, let you control several properties:

- *Operation mode*: defines how the router updates its neighbors. By default, demand-dial interfaces are set to auto-static update, and LAN interfaces are set to periodic updates.
- *Outgoing packet protocol*: determines how packets are sent. If you have all RIPv2 routers on your network, the RIP version 2 multicast option is the most efficient. Other options exist for networks that use RIPv1 or a mix of RIPv1 and RIPv2. A final option, Silent RIP, lets your router listen for and accept updates from other routers without sending its own updates.
- *Incoming packet protocol*: specifies what kinds of RIP packets your router accepts from other routers.
- *Added cost for routers*: lets you control how much this router increases the hop count added to other router's routing tables. The higher you set the cost, the less likely your router will be used.
- *Tag for announced routes*: lets you supply a tag to be included in RIP updates. RRAS does not use this feature, but other routers may.
- *Activate authentication* and *password*: provide some security for your router. Once you turn on authentication, other routers must be configured with the same password in order to exchange information.

Security Properties The Security page for the RIP interface, shown in Figure 7-23, lets you add restrictive properties to your router. First, select an action from the drop-down menu to specify whether the restrictions apply to incoming or outgoing packets. Next, select whether to accept all routes (or announce all routes for outgoing packets), accept only those in the specified ranges, or reject those in the specified ranges. Finally, specify the ranges to which the option applies.

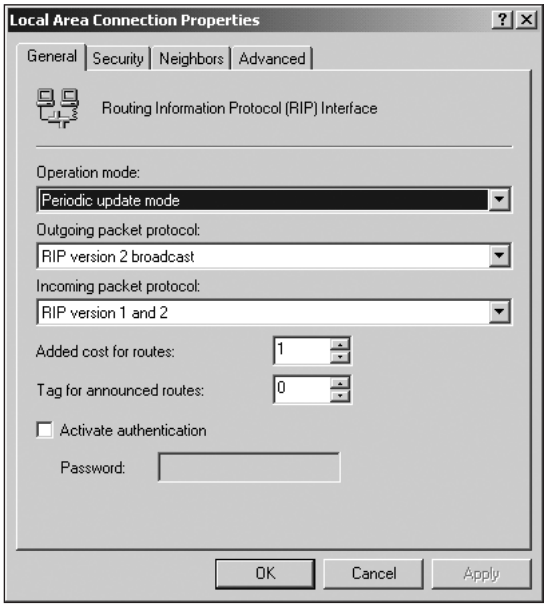

Figure 7-22 General page of the RIP interface

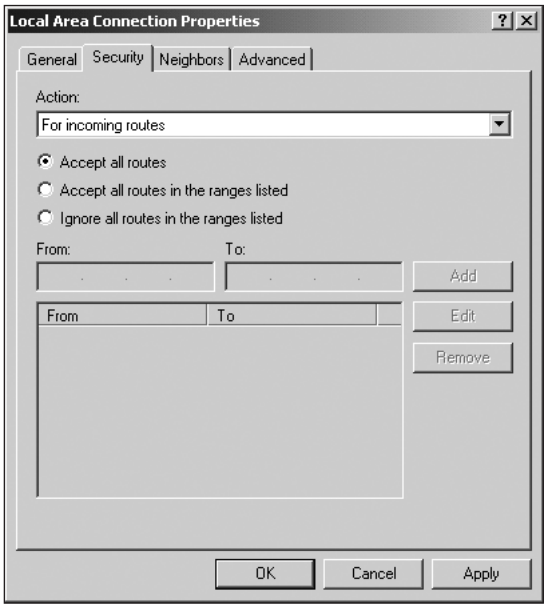

Figure 7-23 Security page for the RIP interface

Neighbors Properties The Neighbors page for the RIP interface, shown in Figure 7-24, lets you choose properties that control how the router interacts with its neighboring routers. By selecting a list of trusted neighbors (by entering IP addresses), you can choose to use those neighbors' routes in addition to, or instead of, broadcast and multicast RIP announcements.

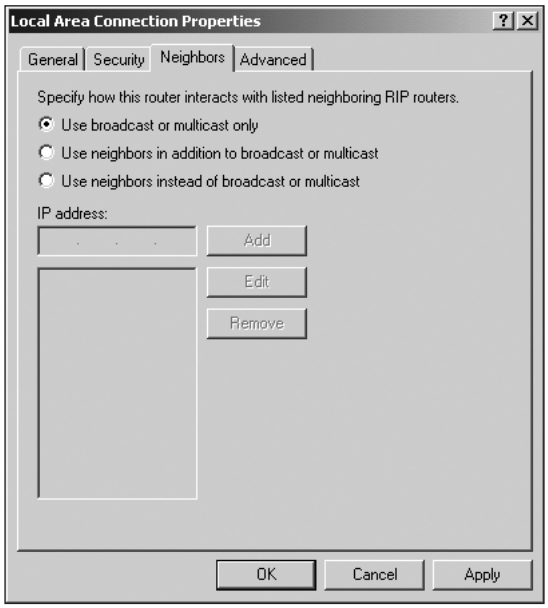

Figure 7-24 Neighbors page of the RIP interface

Advanced Properties The Advanced page lets you set a number of properties that you may never need to worry about, but will need to know for the exam. Table 7-3 lists and describes these properties.

Table 7-3 Advanced properties for a RIP interface

Available pages	Use
Periodic announcement interval	Controls the interval at which periodic router announcements are made; works in conjunction with the Operation mode set in the General page
Time before routes expire	Controls how long the route may stay in the routing table before it expires; routes destined to expire can be refreshed if another router sends the route again
Time before route is removed	Controls how much time may pass between the time a route expires and its removal from the table

Table 7-3 Advanced properties for a RIP interface (continued)

Available pages	Use
Enable split-horizon processing	Enables the router to not rebroadcast routes learned from a specific network back onto that network; this helps prevent loops from occurring
Enable poison-reverse split horizon	Modifies the way split-horizon processing works; with poison-reverse enabled, routes learned from a network are rebroadcast back to that network with a hop count of 16, a special value that tells other routers that the route is unreachable; also helps prevent looping while keeping routing tables up-to-date
Enable triggered updates	Controls whether you want routing table changes to be sent immediately when they are noticed
Send clean-up-updates when stopping	Controls whether RRAS sends announcements that mark the routes it was handling as unavailable when the service stops
Turn on host routes in received announcements	By default, RRAS ignores any host routes it sees in RIP announcements; with this property RRAS sees those routes instead
Include host routes in sent announcements	Directs RRAS to send host route information as part of its RIP announcements; off by default
Process default routes in received announcements and Include default routes in sent announcements	Properties that work the same way as the host routes properties defined above
Disable subnet summarization	When off, RIP doesn't advertise subnets to routers on other subnets; only available with RIPv2

OSPF Interface Properties

The following property pages are available: General, NBMA Neighbors, and Advanced.

General Properties The General page for the OPSF interface, shown in Figure 7-25, has a number of properties. These include:

- *Enable OSPF for this address*: along with the address drop-down list, controls whether OSPF is active at the selected address. Since a single interface can have multiple IP addresses, you can use this drop-down list to specify which addresses are and are not OSPF-capable.
- *Area ID*: drop-down list lets you select to which OSPF area this interface belongs. Each IP address assigned to the interface can be in a separate area.
- *Router priority*: controls the priority of the interface relative to other routers in the area. The router with the highest priority in an area is the preferred router for the area.

- *Cost*: controls the hop count cost associated with the interface.
- *Password*: works just like it does for RIP. Any routers configured with the same password can communicate.
- *Network type*: controls how the router interacts with other routers. A broadcast router can communicate with any number of other routers. A point-to-point router communicates with only one other router. A **non-broadcast multiple access (NBMA) router** communicates with multiple other routers without using a broadcast. If you set up your router as an NBMA router, you can set additional properties using the NBMA Neighbors page.

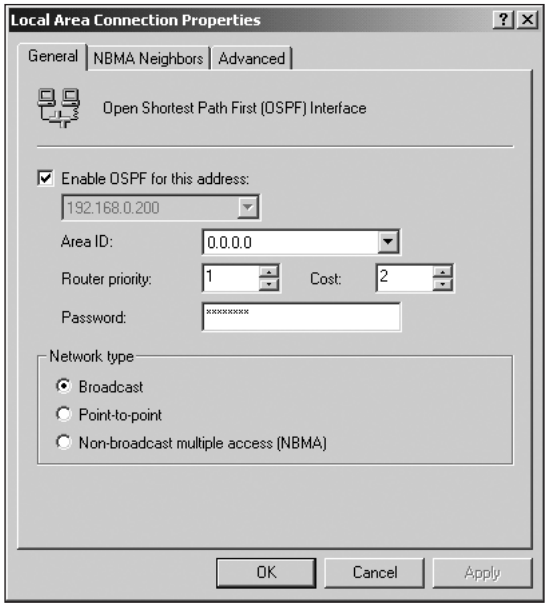

Figure 7-25 General page of the OPSF interface

NBMA Neighbors Properties The NBMA Neighbors page shown in Figure 7-26, lets you choose the neighboring routers with which you want your router to communicate if it is set up as an NBMA router. Just use the IP address drop-down menu to select the IP address for which you want to configure neighbors. (Remember that an interface can have more than one IP address.) For each IP address, enter the IP addresses of the routers you want to configure as neighbors. For each neighbor, you can also set a router priority relative to other neighbor routers.

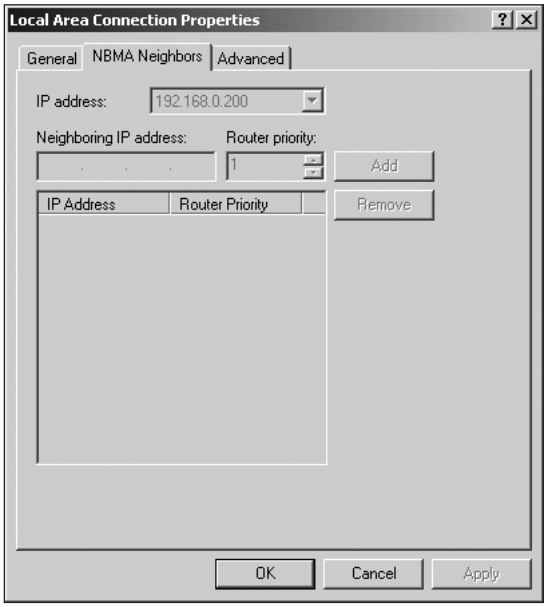

Figure 7-26 NBMA Neighbors page of the OPSF interface

Advanced Properties The Advanced page for the OSPF interface holds six miscellaneous properties. At the top of the page, you can choose the IP address for which you want to configure properties. You can apply different properties to different IP addresses, including:

- *Transit delay*: controls how long it should take for a link-state update to propagate from the router. This information helps other routers determine how fresh information is.
- *Retransmit interval*: controls the estimated round-trip delay when two routers communicate. If the round trip takes longer than this interval, communications are retransmitted.
- *Hello interval*: controls how often routers send packets to discover other routers on the network. You must set the same value for all routers on the network.
- *Dead interval*: controls how long peers wait before they mark a non-responding router as dead. Microsoft recommends using an integral multiple of the Hello interval for this setting. For example, if you set the Hello interval to 10 seconds, you should set the Dead interval to 20, 30, 40, and so on.
- *Poll interval*: controls how long an NBMA router waits before attempting to contact an apparently dead router to see if it is really dead. Microsoft recommends setting this to at least twice the Dead interval.
- *Maximum transmission unit (MTU) size*: specifies how big an OSPF packet can be.

MONITORING IP ROUTING

The RRAS snap-in has a number of displays for monitoring the status of various components. You already saw a few of these displays in this chapter, including:

- *Server Status*: displays the state and type of each RRAS server, as well as the number of ports configured and the number of users connected.
- *General container inside the IP Routing container*: displays all interfaces configured on the server. These include both LAN and demand-dial interfaces. Also displays the state of the interface (up or down) and the IP address associated with the interface.
- *Static Routes container*: displays all static routes added manually to the routing table. Right-clicking the Static Routes container and choosing the Show IP Routing Table command opens a dialog with a more complete version of the routing table that includes the default routes created by Windows 2000.
- *Dynamic routing protocol containers (RIP and OSPF)*: displays the interfaces associated with the protocols and various statistics about each interface's use.

In addition, you may find a few other displays helpful in monitoring and troubleshooting your IP routing implementation. These include:

- *IP Routing Statistics*: include the number of routes in the routing table, the number of IP and UDP datagrams forwarded and received, and the number of connection attempts. To display routing statistics, right-click the General container and choose the Show TCP/IP Information command.
- *Router Status*: displays how many bad packets and bad routers each router tried to send to your RRAS server. To view existing RIP neighbors, right-click the RIP container and select the Show Neighbors command.
- *Defined Areas*: lists the state of the area (up or down) and the number of shortest-path computations performed. To see the list of all defined areas, right-click the OSPF container and select the Show Areas command.
- *Link-State Database*: displays the entire contents of the link-state database. To view the contents, right-click the OSPF container and select the Show Link-State Database command.
- *List of Neighbors*: displays each neighbor's type (broadcast, point-to-point, or NBMA) and state. Right-click the OSPF container and select the Show Neighbors command to see a list of neighbors.

Hands-on Project 7-5 at the end of the chapter details steps for monitoring router status.

CHAPTER SUMMARY

- IP Routing is the method that the IP protocol uses to transfer data between computers on a network. In Windows 2000, the Routing and Remote Access Service (RRAS) supports IP routing. Direct routing occurs when both the source and destination hosts are on the same network segment. Indirect routing occurs when the source and destination hosts are not on the same network segment and packets must pass through a router.
- A router is a physical device used to connect a number of network segments. Routers can be dedicated pieces of hardware, or they can be computers with more than one network adapter card, each connected to a different network segment.
- On a static router, you must enter routing tables manually. A static router only knows about networks directly connected to it or networks that you tell it about. Dynamic routers are routers that have some automatic method of sharing their routing information with other routers on the network. If routing or network information changes, a router automatically updates its routing tables and forwards that information to other dynamic routers that it knows about.
- A dynamic routing protocol used to connect two routers in the same autonomous system is called an interior routing protocol. Windows 2000 supports two interior dynamic routing protocols: Routing Information Protocol (RIP) versions 1 and 2 and Open Shortest Path First (OSPF). RIP is a distance vector routing program, meaning that it not only supplies information about the networks a router can reach, but supplies information about the distances to these networks as well. This distance simply reflects the number of routers a packet must cross, or hop, to reach a particular network.
- OSPF is a link-state routing protocol that enables routers to exchange routing information. It is called a link-state protocol because it actually creates a map (a routing table) of the network that calculates the best possible path to each network segment by maintaining information on the state of links (whether they are up or down).
- Exterior routing protocols are used to exchange routing information between networks that are not autonomous (that is, do not share a common administration). The first exterior routing protocol developed was the Exterior Gateway Protocol (EGP). Since then, a newer and more powerful exterior routing protocol has been developed: the Border Gateway Protocol (BGP).
- Enabling routing on a Windows 2000 server is a three-step process. First, you must enable the RRAS service. Next, you must install and configure any routing protocols (RIP or OSPF) if you want your new router to function as a dynamic router. If you do not, you can configure static routing instead. Finally, you must give each routable interface on the server (network adapter card or demand-dial) a network address for each protocol you allow to be used over the interface. If you want to use demand-dial routing, you must also configure a demand-dial interface.

KEY TERMS

Address Resolution Protocol (ARP) — Low-level protocol that resides within the IP protocol. It is used as a way of resolving IP addresses to MAC addresses.

area border routers — OSPF router that has an interface in more than one OSPF area.

areas — OSPF division of the internetwork into collections of contiguous networks that help keep routing tables from growing too large. Each router only keeps a link-state database for those areas connected to the router.

autonomous system — One in which a set of networks and routers are all under the same administration.

backbone area — OSPF areas connected by a special type of area called a backbone area.

backbone router — Any router configured in an OSPF backbone area.

Border Gateway Protocol (BGP) — Newer and more powerful exterior routing protocol that has largely replaced the older Exterior Gateway Protocol.

converged — Status of an internetwork when all its routers have the correct routing information in their tables.

Convergence time — When a link or router fails, the time taken for all routers on the network to reconfigure themselves with the proper information.

default gateway — Defined on most TCP/IP hosts and simply a router where a packet is sent if its destination network is not found in a routing table.

demand-dial interfaces — Interface configured in RRAS that can dial a remote router whenever a connection needs to be made.

dynamic router — Routers that automatically share their routing information with other routers on the network using a router protocol such as RIP or OSPF.

Exterior Gateway Protocol (EGP) — Exterior routing protocol used to connect different autonomous systems.

hop — Each router that a packet of information must pass between its source and destination hosts. The number of hops is also referred to as metric count or metric cost.

indirect routing — Occurs when a packet of information must pass over a router at some point between its source and destination.

IP (Internet Protocol) — Network layer protocol of the TCP/IP protocol suite that is responsible for routing packets between hosts.

MAC address — Physical address of a network interface. The Address Resolution Protocol is responsible for translating between MAC and IP addresses.

multihomed — Describes a computer with an interface on more than one network.

non-broadcast multiple access (NBMA) router — Router that can communicate with other routers without broadcasting.

Open Shortest Path First (OSPF) — Link-state routing protocol that enables routers to exchange routing information. Called a link-state protocol because it actually creates a map (a routing table) of the network that calculates the best possible path to each network segment by maintaining information on the state of links (whether they are up or down).

RIPv1 — Simple-to-use and well-supported interior routing protocol. RIP is a distance vector routing program, meaning that it not only supplies information about the networks a router can reach, but supplies information about the distances to those networks as well.

RIPv2 — Protocol developed to address several shortcomings in RIPv1, for example, by providing a multicast option in addition to broadcasts for routing announcements and by including the subnet mask in announcements.

ROUTE command — Command-line utility used to manipulate static entries in a routing table.

routing table — List of networks that the system knows about and the IP addresses of routers that packets must pass through to get to those networks.

static router — Router to which routes must be added manually using either the ROUTE command or the RRAS snap-in.

Review Questions

1. Which of the following can you use for a demand-dial interface? (Choose all that apply.)
   a. Modem
   b. Parallel port
   c. VPN port
   d. Ethernet adapter
2. You have three network adapters in your RRAS server, each with a separate IP address. You plan to use two different routing protocols. How many default gateways must you define on the server?
   a. 1
   b. 2
   c. 3
   d. 6
3. Routing table entries usually contain which of the following? (Choose all that apply.)
   a. Destination address for a remote network
   b. Metric for the router
   c. Date and time of the route's creation
   d. Forwarding address for remote traffic
4. A _____ is a connection that brings up a link when it's needed to pass packets.
5. ARP is an example of an exterior routing protocol. True or false?

6. How do you configure router discovery messages?
   a. Through the General page of the LAN interface properties
   b. Through the Discovery page of an OSPF or RIP interface properties
   c. Through the General page of an OSPF or RIP interface properties
   d. By adding an input filter that rejects them
7. An RRAS server can only support one networking protocol on a system. True or false?
8. You use OSPF on a router on your local area network. How should you configure the router?
   a. As a point-to-point router
   b. As an NBMA router
   c. As a broadcast router
   d. As a multicast router
9. Which of the following statements is true of a border router?
   a. It acts as a gateway between routing areas.
   b. It routes traffic internal to an area.
   c. It cannot be used with RRAS.
   d. None of the above.
10. You can manually update a dynamic router's routing table. True or false?
11. _____ refers to the amount of time all routers on the network take to reconfigure themselves after a link or router fails.
12. Which of the following protocols are forms of interior routing protocols? (Choose all that apply.)
    a. RIP
    b. EGP
    c. OSPF
    d. VPN
13. _____ is an example of a vector-based routing protocol.
14. Which of the following refers to an OSPF router that has an interface on more than one network?
    a. Backbone router
    b. Dynamic router
    c. Area border router
    d. Area router
15. _____ is the primary advantage of OSPF over RIP.

16. Which of the following switches do you use with the ROUTE command to remove all entries from a static routing table?
    a. -f
    b. -r
    c. -d
    d. -remove
17. _____ is the local loopback IP address used for testing IP configurations.
18. You can configure a password for both RIP and OSPF routers. True or false?
19. You want to configure your OSPF router *not* to advertise routers it finds outside your system. Where would you do this?
    a. The General page of the IP Routing container's properties
    b. The General page of the OSPF container's properties
    c. The General page of an OSPF interface's properties
    d. The General page of the Static Routes container's properties
20. Windows 2000 supports both the EGP and BGP exterior routing protocols. True or false?

HANDS-ON PROJECTS

All Hands-on Projects in this chapter require at least one server computer set up as described in the lab set-up section in the front of this book. To complete these exercises, you must have completed the projects in Chapters 2 and 3 on installing networking protocols and configuring DHCP.

Project 7-1

To install the Routing and Remote Access Service, follow these steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then select **Routing and Remote Access**.
2. Right-click the computer name and select **Configure and Enable Routing and Remote Access** from the context menu.
3. On the Welcome screen for the Routing and Remote Access Server Setup Wizard, click **Next**.
4. On the Common Configuration screen, select the **Network Router** option and then click **Next**.
5. On the Remote Client Protocols screen, under Protocols, make sure that TCP/IP is listed.
6. Verify that **Yes, all the required protocols are on this list** option is selected, and click **Next**.

7. On the Demand-Dial Connections page, choose the **Yes** option.
8. On the IP Address Assignment screen, make sure that the **Automatically** option is selected and then click **Next**.
9. Click **Finish**.

Project 7-2

To add and remove static routes with the RRAS snap-in, follow these steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then select **Routing and Remote Access**.
2. Find the server you want to configure in the left pane, and expand it.
3. Find the **IP Routing** container under that server, and expand it.
4. Right-click the **Static Routes** container, and choose the **New Static Route** command from the shortcut menu.
5. Select the interface you want to use from the Interface drop-down list.
6. Enter a **destination address** for the network you want to route to and a **subnet mask**.
7. In the Gateway field, enter the **IP address** of your RRAS server.
8. Click **OK** to close the Static Route dialog box.
9. Right-click the **Static Routes** container, and select the **Show IP Routing Table** command from the shortcut menu.
10. In the dialog box that opens, verify that the new route you just added is in the table.
11. Click the **Close** button to close the dialog.
12. Highlight the **Static Routes** container.

    Notice the routing table in the right pane.
13. Right-click the **static route** you just created, and select **Delete** from the shortcut menu to remove it from the table.

Project 7-3

To install a dynamic routing protocol, follow these steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then select **Routing and Remote Access**.
2. Find the server you want to configure in the left pane, and expand it.
3. Find the **IP Routing** container under that server, and expand it.
4. Right-click the **General** container and select **New Routing Protocol** from the shortcut menu.
5. Select the **RIP Version 2 protocol** from the list, and click **OK**.

6. Right-click the **General** container again, and select **New Routing Protocol** from the shortcut menu.
7. Select the **Open Shortest Path First (OSPF)** protocol from the list, and click **OK**.

   The RRAS display should update to show the two new protocols inside the IP Routing container.

Project 7-4

To create a new demand-dial interface, follow these steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then select **Routing and Remote Access**.
2. Right-click **Routing Interfaces**, select **New Demand-Dial Interface** from the shortcut menu, and click **Next**.
3. In the Interface Name field, type a **name** for the remote router to which you will connect, and click **Next**.
4. Select **Connect using a modem**, **ISDN adapter**, or **other physical device**, and click **Next**.
5. If your system contains more than one network adapter, select the **physical device** that the interface will use, and click **Next**.
6. If you choose to connect using the modem in Step 4, you are now shown a Phone number page. Enter the number of the router to which you want to connect.
7. On the Protocols and Security page, make sure that only the **Route IP Packets** option is selected and click **Next**.
8. On the Dial-Out Credentials page, enter the **user information** needed to connect to the remote router and click **Next**.
9. Click **Finish**.

Project 7-5

To monitor the status of IP routing, follow these steps:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then select **Routing and Remote Access**.
2. Expand the server whose status you want to monitor in the left pane.
3. Select the **Routing Interfaces** container.

   Note that the right pane now lists all the interfaces available on the server along with their connection state.
4. Select the **General** container beneath the IP Routing container.

   The right pane displays the IP routing interfaces and their status.

5. Right-click the **General** container and choose the **Show TCP/IP information** command.

   Check the number of IP routes shown.

6. Right-click the **Static Routes** container, and select the **Show IP Routing Table** command.

   This displays all routes available in the routing table.

CASE PROJECTS

Case 1

Your company network consists of four subnets configured with the following network IDs:

- 192.168.0.0
- 192.168.1.0
- 192.168.2.0
- 192.168.3.0

You plan to configure a single RRAS server with four network adapters as the single router on this network. Sketch a network diagram showing how you will configure the network. Include an IP address for each of the four interfaces on the RRAS server.

Case 2

Your network has grown steadily, and you decided to implement several more network segments. You propose moving to a dynamic routing system, and your supervisor seems interested. In response to her request, prepare a list showing the advantages and disadvantages of using RIPv1, RIPv2, and OSPF.